THE HONORABLE TANA LIN

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

DOMINIC MAYHALL, individually and on behalf of all others similarly situated,

Plaintiff,

v.

AMAZON WEB SERVICES INC., *et al.*,

Defendants.

Case No.: 2:21-cv-1473-TL-MLP

DEFENDANTS' MOTION TO DISMISS FIRST AMENDED COMPLAINT

NOTE ON MOTION CALENDAR: MAY 10, 2024

ORAL ARGUMENT REQUESTED

FENWICK & WEST LLP
401 UNION STREET, 5TH FLOOR
SEATTLE, WASHINGTON 98101

TABLE OF CONTENTS

FENWICK & WEST LLP
401 UNION STREET, 5TH FLOOR
SEATTLE, WASHINGTON 98101

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

On October 29, 2021, Plaintiff Ann Mayhall filed this action on behalf of her then sixteen-year-old son Dominic, who used a "Scan Your Face" feature to create a personalized character in the basketball simulation video game NBA 2K, which is owned and operated by Take-Two Interactive Software, Inc. and/or its wholly owned subsidiary 2K Games, Inc. (collectively, "Take-Two"). Dominic voluntarily took pictures of his face through the NBA 2K's companion smartphone application ("NBA2K App") and affirmatively consented to create a "MyPLAYER" avatar superimposing those photos onto a player in the game.

Defendants Amazon Web Services, Inc. ("AWS") and its corporate parent Amazon.com, Inc. ("Amazon"),[1] were never alleged to have interacted with Dominic. Instead, Plaintiff's original Complaint speculated that both Defendants violated the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 ("BIPA"), by "us[ing] their computing power not only to collect facial features vectors from face-scan data for Take 2 but also to construct a 3D Face Geometry of the user, which Defendants then transmit to the players' Gaming Platforms." Dkt. No. 1 ¶¶ 106-07. The Court relied upon this allegation in denying Defendants' motion to dismiss the Complaint. Dkt. No. 49 at 6, 9, 11. Specifically, this Court held that this allegation was sufficient to plead the necessary element of control over biometric data necessary to establish "possession" and "collection" under BIPA. Report and Recommendation ("R&R"), Dkt. No. 31, p. 14; Dkt. 49, p. 5. But this allegation was false and has now been withdrawn. For this and other reasons described below, the Amended Complaint fails to state claims under BIPA and should be dismissed.

In the Amended Complaint, Plaintiff is now Dominic Mayhall (rather than his mother), and he no longer alleges that either AWS or Amazon collects or transfers any data from the "Scan Your Face" feature, or that the alleged "capturing and/or creation of biometric data of the user" was performed using Defendants' cloud servers. Dkt. No. 72 ("Am. Compl.") ¶¶ 100, 107. Indeed,

[1] As Defendants' counsel has repeatedly informed Plaintiff, Amazon.com, Inc. is not a proper defendant. It is a holding company with no customers or equipment of its own. Amazon.com, Inc. has provided a verified interrogatory response confirming that it had no role in any of the alleged acts or occurrences in the Complaint, a fact that remains true for allegations in the Amended Complaint.

Plaintiff now ***admits*** that the "computing power" used to construct 3D Face [redacted][2] not from AWS or Amazon. *Id*.

Instead of alleging that AWS or Amazon captured or collected Plaintiff's facial geometry, which was central to this Court's denial of Defendants' prior motion to dismiss, Plaintiff now alleges—for the sole purpose of online multiplayer games ("Online Games")—[redacted]. Based solely on these allegations, Plaintiff alleges AWS and Amazon violated Sections 15(a), (b), and (d) of BIPA.

The Court should dismiss each of these claims because Plaintiff has failed to plausibly allege any facts to show that AWS or Amazon possessed, collected, or disclosed his biometrics as required to state a claim under BIPA.

First, claims asserted pursuant to BIPA Sections 15(a) and 15(d) may be maintained only where a private entity allegedly "possesses" biometric information. This Court previously agreed that "possession" for purposes of BIPA requires that a defendant ***exert control*** over the alleged biometric data. R&R, Dkt. No. 31, p. 14; Dkt. 49, p 5. In denying Defendants' motion to dismiss Plaintiff's original Complaint, the Court found that the possession element was satisfied by allegations that Defendants "uploaded the photos it collected from [Plaintiff's child] to its AWS account, extracted face geometry data from them ***using AWS computer power***, and ***then stored*** the resulting face geometry data in its AWS account." Dkt. No. 49, p. 6 (emphasis added). The Amended Complaint abandons these allegations, such that Plaintiff ***no longer alleges*** that either AWS or Amazon uploaded photos, extracted face geometry, actively stored face geometry data in an AWS cloud server, or otherwise exercised any control over Take-Two's MyPLAYER data. The Amended Complaint confirms that this action was filed and maintained based on speculative and completely unfounded allegations that Plaintiff now recants. Because the Amended Complaint no

[2] Gaming Platform is defined in the Amended Complaint to include video game consoles such as the Xbox, PlayStation and Nintendo Switch, as well as personal computers. Am. Compl. ¶ 82.

longer alleges "possession" as required to maintain a claim under Sections 15(a) or 15(d), both claims should be dismissed.

Second, Plaintiff's Section 15(b) claim fares no better. Section 15(b) requires "that a defendant entity must take active steps" to collect, capture or obtain biometric information. R&R, Dkt. No. 31, p. 20. The Court previously found the "active step" requirement satisfied by allegations that Defendants' computing power extracted facial geometry from Plaintiff's photos. Dkt. No. 49, p. 9. But again, that unfounded allegation has been excised from the Amended Complaint. The remaining allegations are insufficient to support any finding of an "active step" and place this case squarely within prior precedents finding that a technology service provider cannot be liable under Section 15(b) for the actions of non-parties utilizing its services. The Amended Complaint contains no allegation that AWS or Amazon even knew that Take-Two was transmitting MyPLAYER data between Gaming Platforms, much less took any "active step" to collect, capture, or obtain that data, or any other alleged biometric information.

Third, at its core, Plaintiff's Amended Complaint seeks to impose BIPA liability on AWS and Amazon for doing nothing more than providing passive cloud services that help customers like Take-Two transmit their content to and among their end users. This interpretation of BIPA runs directly contrary to Section 230 of the Communications Decency Act ("CDA"), 47 U.S.C. § 230 (1996), which grants immunity to providers of "interactive computer services" with respect to state laws that would create obligations to monitor third-party content. *See HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 681 (9th Cir. 2019). Neither AWS nor Amazon owns or controls the content at issue (or even has the right to access it). Under these circumstances, Illinois courts have recognized that BIPA does not, and cannot, apply. *See Kyles et al. v. Amazon Web Services, Inc.*, 2021-CH-04026 MTM (Ill. Cir. Ct. Jan 4, 2023) (bench ruling attached as Exhibit A, dismissing BIPA claims against AWS as a cloud service provide based on an absence of control (35:24-36:3)); *Clark v. Microsoft Corp.*, 2023 WL 5348760, at *3 (N.D. Ill. Aug. 21, 2023) (finding a cloud service provider did not take an "active step" to collect data as required to support a 15(b) claims). And for good reason: cloud service providers have no relationship with their customers' end users and no control over what data their customers choose to collect, transmit, or store in their

accounts. Extending BIPA to cover passive cloud services would thus violate BIPA's plain language (which requires active collection and/or control) and impose impossible burdens that would chill commerce in Illinois. *See Rosenbach v. Six Flags Ent.*, 129 N.E.3d 1197, 1207 (Ill. 2019) (finding compliance with BIPA "should not be difficult" and "whatever expenses a business might incur to meet the law's requirements are likely to be insignificant.") Indeed, it is simply not plausible to expect cloud service providers to police the contents of trillions of customer files (assuming they even had the contractual right to do so) to somehow determine whether they contain biometric information covered by BIPA. And doing so would create a host of other privacy issues. In short, the Court should dismiss the Amended Complaint because Plaintiff's claims stretch BIPA far beyond its language and the legislature's intent.

FACTUAL BACKGROUND[3]

A. The Illinois Biometric Information Privacy Act

The Illinois General Assembly enacted BIPA in 2008 to address the growing use of biometric technology "in the business and security screening sectors" in Illinois. 740 ILCS 14/5(a). The General Assembly found "[m]ajor national corporations ha[d] selected the City of Chicago and other locations in [Illinois] as pilot testing sites for new applications of biometric facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b). The Illinois legislature also found consumers had concerns about "use of biometrics when such information is tied to finances" and were "deterred from partaking in biometric identifier-facilitated transactions," in part because of the "limited State law regulating the collection, use, safeguarding, and storage of biometrics." 740 ILCS 14/5(d), (e). BIPA addresses these concerns by regulating the collection, possession, and storage of certain biometric identifiers and information, while expressly excluding coverage of other data. The statute defines "biometric identifier" using a short, exclusive list of personal data: "'[b]iometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

[3] For purposes of this motion, AWS and Amazon accept all factual allegations as true, but do not "accept as true [] legal conclusion[s] couched as [] factual allegation[s]." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Defendants expressly reserve their right to challenge all facts alleged in the Amended Complaint.

Section 15(a) states that private entities "***in possession*** of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information …." 740 ILCS 14/15(a) (emphasis added).

Section 15(b) requires private entities that "collect, capture, purchase, receive through trade, or otherwise obtain a person's ... biometric identifier or biometric information" to first (1) inform the person of that collection "in writing"; (2) inform the person "in writing of the specific purpose and length of term" regarding the collection; and (3) obtain a "written release" from the person. 740 ILCS 14/15(b).

Finally, Section 15(d) prohibits any private entity "***in possession*** of a biometric identifier or biometric information" to "disclose, redisclose, or otherwise disseminate a person's ... biometric identifier or biometric information" unless the subject of the biometric identifier or information "consents to the disclosure or redisclosure." 740 ILCS 14/15(d) (emphasis added).

B. Take-Two's NBA 2K Video Game

Plaintiff alleges that he played NBA 2K, a basketball video game created and operated by Take-Two. Am. Compl. ¶¶ 75, 186-187. Plaintiff alleges he used the NBA2K App created by Take-Two to scan his face and create a "MyPLAYER" avatar that would resemble his likeness within NBA 2K. *Id.* ¶¶ 88, 189. The information collected through Take-Two's NBA2K App [redacted]. *Id.* ¶¶ 100-101. Take-Two received informed written consent, prior to collecting any information from players, before they created a MyPLAYER. *Id.* ¶ 96. The NBA 2K game, [redacted]. *Id.* ¶ 107. [redacted], players are given the opportunity to review and edit the avatar to better match their appearance, including changing the placement of the ears, eyes, eyebrows, and the shape of the skull. *Id.* ¶ 105.

Critically, the Amended Complaint omits all prior allegations regarding: (1) Defendants' involvement with the collection or transmission of image data through the App; and (2) utilization

of Defendants' computing power to create the MyPLAYER avatar. Plaintiff now concedes that neither AWS or Amazon are involved with the collection of biometric data, the creation of the MyPLAYER avatar, or storage of the MyPLAYER avatar for use in offline gaming.

C. Defendants' Alleged Conduct

Defendants' involvement—according to the Amended Complaint—occurs only after the MyPLAYER avatar has been generated, edited, and accepted by the player. If a player chooses to play against opponents through an internet connection, Take-Two allegedly [redacted]. *Id*. ¶¶ 132-33. [redacted] *Id*. ¶¶ 134-149. Plaintiff further speculates [redacted]. *Id*. However, this allegation is directly contradicted by the witness declaration upon which Plaintiff bases his Amended Complaint.[4] In that same declaration, [redacted]. *See* Ex. B, Decl. of Erick Boenish, ¶ 46. Based on these allegations, Plaintiff asserts that AWS and Amazon violated BIPA Sections 15(a), (b), and (d).

Notably, Plaintiff does not allege either AWS or Amazon have any control over what data Take-Two sends through AWS servers, or whether players like Plaintiff elect to use their MyPLAYER avatar in Online Games. Plaintiff also does not allege that AWS or Amazon ever: (1) collected or stored MyPLAYER data, (2) accessed MyPLAYER data, (3) used MyPLAYER data for their own purpose, or (4) even ***knew about*** MyPLAYER data prior to this lawsuit. Plaintiff further admits that, pursuant to AWS's Customer Agreement, Defendants lack the discretion to access or use Take-Two's data for their own purpose and may only access the data to fulfil their

[4] Plaintiff's reference in footnote one of the Amended Complaint to 2023 testimony refers to the Declaration of Erick Boenish furnished by Take-Two in this matter. *See Dunn v. Castro*, 621 F.3d 1196, 1205 n.6 (9th Cir. 2010) (under "incorporation by reference" doctrine, court may consider "documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the [plaintiff's] pleading") (alteration in original) (citation omitted).

contractual obligations to Take-Two or as required by law or law enforcement agencies. *Id.* ¶ 157. Nor do Defendants have the authority to move or replicate data outside of a region without express consent of their customers (here, Take-Two) or if otherwise required by law. *Id.* ¶¶ 158-159. Consistent with Plaintiff's allegations, Take-Two's representative testified [redacted] Ex. B, ¶ 45 (emphasis added).

ARGUMENT

Rule 12(b)(6) requires dismissal when a plaintiff "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). To state a claim, allegations must be more than "speculative," "conceivable," and possible; instead, they must be facially "plausible." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-57, 570 (2007). Although a district court accepts well-pleaded allegations as true, it must disregard "legal conclusions" and other "conclusory statements," fully scrutinizing allegations to ensure that they are truly plausible and not "'merely consistent with' a defendant's liability." *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009) (citation omitted). The plausibility requirement is not satisfied by a "formulaic recitation of the elements of a cause of action." *Id.* at 678; *see Landers v. Quality Commc'ns, Inc.*, 771 F.3d 638, 644 (9th Cir. 2014), *as amended* (Jan. 26, 2015).

Under the "incorporation by reference" doctrine, for a 12(b)(6) motion, courts may consider "documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the [plaintiff's] pleading." *Dunn v. Castro*, 621 F.3d 1196, 1205 n. 6 (9th Cir. 2010); *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007) (courts "ordinarily examine . . . matters of which the court may take judicial notice" when ruling on a Rule 12(b)(6) motion); *see also Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005) (incorporating by reference complete copies of websites where the complaint included only excerpts because [i]n evaluating the context in which the statement appeared, we must take into account 'all parts of the communication that are ordinarily heard or read with it.").

I. PLAINTIFF'S SECTION 15(A) AND 15(D) CLAIMS FAIL BECAUSE NEITHER AWS NOR AMAZON POSSESS HIS BIOMETRIC DATA.

A. BIPA Section 15(a) and 15(d) Claims Require Possession of Biometric Data.

Section 15(a) of BIPA requires that any "private entity" that is "in possession of" biometric information or identifiers must develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometrics.[5] 740 ILCS 14/15(a). Similarly, Section 15(d) applies only to private entities "in possession" of biometric data and prohibits disclosure or dissemination of it without consent. 740 ILCS 14/15(d).

BIPA does not define "possession." 740 ILCS 14/10. When interpreting BIPA, Illinois courts "'assume[] that the legislature intended for the term to have its popularly understood meaning,' or its 'settled legal meaning' if one exists." *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) (quoting *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019)) (brackets omitted).

The Illinois Supreme Court has held that "'possession,' as ordinarily understood, occurs when a person has or takes control of the subject property or holds the property at his or her disposal." *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005). The touchstone of "possession" is the exercise of ***control*** over the biometric information. *Id.*; *see also Honeywell Int'l, Inc. v. Dep't of Revenue of State of Ill.*, 851 N.E.2d 79, 85 (Ill. App. Ct. 2006) (finding that one does not possess an item "unless he has the ability, at a given time, to exercise dominion and control over [it]"). Nothing in BIPA alters this ordinary definition of "possession." *Heard*, 440 F. Supp. 3d at 968.

Section 15(a) and 15(d) claims must be dismissed when a plaintiff fails to allege facts showing that the defendant controlled the biometric data at issue. For example, in *Heard*, the plaintiff sued Becton Dickinson ("BD"), the manufacturer of a medication-dispensing system accessed through a fingerprint scan and used by the hospitals where plaintiff worked. *Id.* at 962. The court dismissed claims under Sections 15(a) and 15(d), reasoning that Heard had "not

[5] BIPA defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" and defines "biometric information" as any information "based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10. Biometric identifiers and biometric information are collectively referred to herein as biometric data or biometrics.

adequately pleaded 'possession' because he fail[ed] to allege that BD 'exercised *any* dominion or control over [his] biometric data.'" *Id.* at 968 (emphasis and second alteration in original). An allegation that BD "subsequently stored [Heard's] fingerprint data in their systems" was insufficient because the "allegation does not plead that BD exercised any form of control over the data or that it held the data 'at [its] disposal.'" *Id.* (citations omitted) (alterations in original); *see also Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C866, 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021) (dismissing Section 15(a) and 15(d) claims in the absence of "factual allegations that plausibly establish that defendant exercised control over plaintiff's data or otherwise held plaintiff's data at its disposal").

Consistent with this Illinois precedent, this Court previously held that "possession 'occurs when a person has or takes ***control*** of the subject property.'" Dkt. No. 31 at p. 14; Dkt. No. 49 at p. 5 (quoting *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005) (emphasis added). In denying Defendants' Motion to Dismiss the original complaint, the Court cited Plaintiff's allegation that Defendants "construct(s) a 3D Face Geometry of the user" as sufficient to allege Defendants had control of biometric information. The Court cited *Wilk v. Brainshark, Inc*., No. 121-cv-4794, 2022 WL 4482842, at *5 (N.D. Ill. Sept. 27, 2022) in which a defendant allegedly scanned and analyzed facial geometry.[6] Unlike the original complaint, however, the Amended Complaint does not allege that either AWS or Amazon has ***any*** involvement in the scanning or construction of facial geometry or otherwise exercised any control over Take-Two's data. Applying the established law to the facts now alleged requires dismissal for a failure to plead control, and therefore possession, as required under BIPA.

B. Plaintiff Fails to Allege Defendants Controlled Any of Take-Two's Alleged Biometric Information.

The Amended Complaint fails to create a plausible inference that either AWS or Amazon exercised any control over Plaintiff's biometric data. To the contrary, read as a whole, Plaintiff's

[6] In its prior Report and Recommendation, Magistrate Judge Peterson also cited to *Naughton v. Amazon.com, Inc.*, 2022 WL 19324 (N.D. Ill. Jan 3, 2022). *Naughton* is inapposite because the plaintiff alleged that his employer actively "***collect[ed] the data for its own use***" and thus controlled it. *Id.* at *3 (emphasis added). Plaintiff does not allege AWS or Amazon collected biometric data for their own use.

Amended Complaint makes clear that AWS is a passive cloud service provider distributing Take-Two's data at the direction of, and for the benefit of, Take-Two and the Plaintiff himself. As an Illinois court found in *Kyles v. AWS,* AWS, as a cloud service, does not possess or control biometric data merely because such data is allegedly stored on its system by the third party. *See* Ex. A (35:24-36:3.) Plaintiff does not allege a single instance of AWS or Amazon ever collecting, transmitting, or storing Plaintiff's data at its own initiative or for its own purpose.

The reason for Plaintiff's failure to allege control is obvious: it does not exist, as Plaintiff's own allegations and the documents incorporated into his Amended Complaint make clear. The sum-and-substance of Defendants' alleged involvement with MyPLAYER data is encapsulated in just three paragraphs of the Amended Complaint, [redacted]. ¶¶ 85-87. Plaintiff follows these allegations with more than forty paragraphs detailing the way data is collected and processed to generate MyPLAYER avatars while ***conceding*** Defendants have nothing to do with that process. *See* ¶ 107. In fact, ***significant portions*** of the Amended Complaint ***have nothing to do with either AWS or Amazon.*** *See, e.g.,* ¶¶ 30-44, 75-80, 88-131, 186-192.

While Plaintiff makes a conclusory allegation that AWS or Amazon retained control over this data, that allegation is flatly contradicted by the facts pleaded in the Amended Complaint.[7] First, Plaintiff cites Section 3.2 of the AWS Customer Agreement which states AWS "will not access or use Your content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." *Id.* ¶ 157. Plaintiff contorts the phrase "except as necessary" to contend AWS retains control, but this tortured reading contradicts the provision's plain meaning. As stated, the ***only*** circumstances under which AWS may access customer data are to (1) fulfill contractual obligations ***to the customer*** (here, Take-Two) or (2) comply with legal requirements and authorities outside of AWS's control. Any reasonable reading of Section 3.2 demonstrates AWS ***lacks control*** of Take-Two's data and cannot simply use it as it sees fit. In fact, an Illinois court recently cited the ***same*** section of the AWS

[7] Plaintiff's allegation of control may be disregarded because they are implausible and amount to a conclusory recitation of the pleading requirements. *See Iqbal*, 556 U.S. at 678-79.

Customer Agreement to find a plaintiff failed to allege AWS controlled biometric data stored on its cloud services. *See Kyles*, Ex. A at 34:7-17.

Likewise, Plaintiff cites language in Defendants' Data Privacy FAQ that states Defendants cannot move the data outside of a region unless: (1) the client who controls the data agrees, or (2) required by law. Again, these restrictions prove that Defendants are ***not*** in control of Take-Two's data. By analogy, if the Internal Revenue Service were to freeze Plaintiff's bank account, no rational factfinder would conclude that the bank—rather than the IRS—is in control of Plaintiff's funds. AWS's relationship to customer data is always at the direction of and for the benefit of the customer, subject to any intervening legal authorities. That is the antithesis of control.

In any event, while Plaintiff alleges that Defendants ***may*** provide customer data to law enforcement and access it under specific circumstances, Plaintiff ***never alleges that this happened*** with any of Take-Two's MyPLAYER data. AWS is the largest cloud computing provider in the world and has vast troves of data on its networks, of which the MyPLAYER data is less than a drop in the bucket. What AWS could theoretically do with Take-Two's data in response to a law enforcement order or Take-Two directive is irrelevant in the absence of concrete allegations.

The bottom line is simple: after many months of discovery, Plaintiff's Amended Complaint does not include a single factual allegation showing that either AWS or Amazon exercised any actual control over Take-Two's MyPLAYER data. AWS is a service provider in the business of providing cloud computing services; it transmits and retains customer data only as necessary to service its clients. That is the reason Take-Two and other entities contract with AWS. The notion that a cloud services provider would exercise control over customer data is fundamentally in conflict with the core function of the industry. Plaintiff's implausible and conclusory assertion of "control" makes no sense and should be disregarded as a matter of law.

The data at issue in this case is, at all times, controlled by Take-Two. *See* Ex. B, Decl. of Erick Boenish, ¶ 45 ("[redacted]") As a cloud services provider, AWS does not own or control its customers' content or data, including any data that Take-Two may collect from its users and store in its AWS account. AWS has ***more***

than one million enterprise customers,[8] eliminating any plausible inference that Defendants even know what is contained in the trillions of files stored on AWS servers. Plaintiff's theory is akin to arguing that a brick-and-motor storage facility owns and controls the possessions customers place in rented storage lockers. Courts have rejected this theory. *See e.g., Street v. Lincoln Safe Deposit Co.*, 254 U.S. 88, 92-93 (1920) (finding a warehouse company "could not sell, give away or otherwise transfer" the lessee's property, and served the limited role of providing protection to the building and its contents); *Dubey v. Pub. Storage, Inc.*, 395 Ill. App. 3d 342, 356, 918 N.E.2d 265, 279 (2009) (affirming punitive damages against a storage facility for conversion of a renter's property); *Jones v. Hanna*, 814 S.W.2d 287, 289–90 (Ky. Ct. App. 1991) (where a storage unit tenant controlled access to unit and facility did not have knowledge of unit's contents, the facility did not possess the contents of the unit). Read in context, Plaintiff's allegation does not come close to plausibly alleging "possession" by Defendants.

Defendants' publicly available agreements and policies make clear that Defendants' customers such as Take-Two own and control their data. *See, e.g.*, AWS Customer Agreement, available at https://aws.amazon.com/agreement/ (last accessed Jan. 7, 2022), attached as Exhibit C, § 14 ("'Your Content' means Content that you or any End User transfers to us for processing, storage or hosting by the Services in connection with your AWS account ...."); [9] *id.* § 3.2 ("We will not access or use Your Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body"); AWS's "Data Privacy FAQ," available at https://aws.amazon.com/compliance/data-privacy-faq/ (last accessed Jan. 7, 2022), attached as Exhibit D ("As a customer, ***you maintain full control of your content*** that you upload to the AWS services under your AWS account, and responsibility for configuring access to AWS services and resources") (emphasis added); *id.* ("As a customer, ***you maintain ownership of your content***, and you select which AWS services can process, store, and host your

[8] *See* AWS Enterprise Solutions, https://aws.amazon.com/enterprise/ (last accessed March 4, 2024).

[9] These documents are expressly cited and relied upon in Plaintiff's Amended Complaint. Dkt. No. 72 ¶¶ 157-58. Even if they were not, citation is appropriate because they are matters of public record and may be considered by this Court in ruling on a motion to dismiss. *See, e.g.*, *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007) (courts "ordinarily examine ... matters of which the court may take judicial notice" when ruling on a Rule 12(b)(6) motion).

content. We do not access or use your content for any purpose without your agreement.") (emphasis added).

AWS contracted with Take-Two—as it does with thousands of other companies—to provide cloud data services for data exclusively owned and controlled by Take-Two. *Ex.* B, ¶¶ 20, 46. No court in Illinois or elsewhere has imposed BIPA liability on a cloud service company that does not own, control, or access data collected by someone else, but merely stores or transmits that data through a server. *See Kyles,* Ex. A (finding AWS, as a cloud service company, does not own or control data collected by a third party stored on its server). Sections 15(a) and 15(d) do not reach AWS's conduct as a third-party vendor with no relationship to Plaintiff whatsoever. To hold otherwise would create absurd results, effectively creating strict liability for all cloud computing service providers who host customer data that unknowingly includes biometric information.

Divorcing possession from actual ***control*** is contrary to Illinois law and would have dire implications for consumers and technology companies, who would have no choice but to cease offering popular services in Illinois given the potential for virtually unlimited liability under BIPA. That is clearly not what the Illinois legislature intended.

Plaintiff's amended allegations reveal the truth—AWS is a passive carrier of data that is at all times generated, controlled, and possessed by non-parties like Take-Two. Plaintiff's Section 15(a) and 15(d) claims should be dismissed.

II. PLAINTIFF FAILS TO STATE A CLAIM UNDER BIPA SECTION 15(B).

A. Plaintiff Does Not Allege Either AWS or Amazon Took Any Active Step to Collect His Biometric Data.

"The key words in a Section 15(b) claim are collecting, capturing, purchasing, or obtaining." *Stauffer v. Innovative Heights Fairview Heights LLC*, No. 3:20-CV-0046-MAB, 2022 WL 3139507, at *3 (S.D. Ill. Aug. 5, 2022). This requires affirmative actions by a defendant above and beyond possession. *See Jacobs*, 2021 WL 3172967, at *2 ("[T]his court concludes that for Section 15(b)'s requirements to apply, an entity must, at a minimum, take an active step to collect, capture, purchase, or otherwise obtain biometric data."); *see also Kyles v. Hoosier Papa LLC*, No. 1:20-CV-07146, 2023 WL 2711608, at *5 (N.D. Ill. Mar. 30, 2023) ("[T]his Court agrees with those cases that hold § 15(b) requires some active step beyond mere possession.").

The Report and Recommendation on Defendant's motion to dismiss Plaintiff's original Complaint cited *Vance v. Amazon.com Inc*., 525 F.Supp.3d 1301 (W.D. Wash. 2021), which did not dismiss a Section 15(b) claim where the defendant allegedly took deliberate actions to obtain and download a data set containing biometrics for its own use. The *Vance* court found this intentional collection qualified as an active step for purposes of Section 15(b). *Id.* at 1312. But Plaintiff's Amended Complaint does not allege ***any*** deliberate act by Defendants to obtain biometric data. More applicable precedent is illustrated by *Jacobs*, 2021 WL 3172967, in which a court dismissed Section 15(b) claims brought against a "third-party technology provider" where the alleged "active collector and processor of the data" was a non-party utilizing the defendant's technology. *Id*. at *3; *see also Clark,* 2023 WL 5348760, at *3 (finding no allegation of an "active step" based on a non-party's alleged use of the defendant's technology to collect biometrics.)

Similarly, the Court previously distinguished *Jones v. Microsoft Corp*., No. 22-cv-3437, 2023 WL 130495 (N.D. Ill. Jan. 9, 2023) based on allegations that are now abandoned in the Amended Complaint. In *Jones*, the court dismissed Jones' 15(b) claim after observing there was no "active-step" by Microsoft when a non-party (like Take-Two) had taken the active steps of collection and sent that data to Microsoft's cloud storage platform. *Id*. at *4. The court found that receiving biometric data incidental to providing cloud storage services did not constitute an "active step" on Microsoft's part to acquire biometric information. The court further noted that Microsoft's contracts with the third-party did not constitute an agreement to receive biometrics through trade, as Microsoft contracted only to receive money in exchange for use of its cloud services and had no interest in the biometric data that its client stored on its platform. *Id*. This Court distinguished *Jones* from its prior decision based on Plaintiff's allegation that Defendants actively collected biometrics from Plaintiff and computed facial scans. As amended, however, Plaintiff's allegations mirror the allegations in *Jones* and warrant dismissal.

B. Plaintiff Concedes AWS and Amazon Did Not Actively Compute or Collect Facial Geometry Data.

Section 15(b) applies only to the private entity that ***actively*** collects, captures, purchases, receives through trade, or otherwise obtains biometrics. The Court's prior ruling turned on

allegations that AWS and Amazon had collected Plaintiff's facial data through the NBA2K App and used its computing power to extract face geometry. Dkt. 49 at p. 9. But AWS or Amazon are no longer alleged to be responsible for either the collection of data or the computation of facial geometry. The alleged collection of Plaintiff's biometric information resulted from Plaintiff's use of the NBA2K App. Take-Two—not Defendants—maintained and operated the NBA2K App, [redacted]. Am. Compl. ¶¶ 11-14. Plaintiff concedes that neither AWS or Amazon has anything to do with Take-Two's App or the collection of alleged biometric data.

The Court specifically relied on Plaintiff's speculative allegation that, to create the MyPLAYER avatar, [redacted] Dkt. No. 1, ¶¶ 105-06; Dkt. 49 at pp. 6, 9. The Amended Complaint removes any assertion of an active step by AWS or Amazon in the collection of data or rendering of facial scans. Am. Compl. ¶¶107-109. Plaintiff now ***admits*** the computational process [redacted] (not on AWS's servers), with ***no involvement*** by AWS or Amazon. *Id*.

The ***active step*** is the linchpin for a Section 15(b) claim. Plaintiff's amended allegations remove the fundamental basis for the Court's prior finding of an active step. Plaintiff has failed to provide facts detailing how AWS, as a cloud services provider, actively collected, captured, purchased, received through trade or otherwise obtained Plaintiff's data. Accordingly, Plaintiff's Section 15(b) claim fails as a matter of law.

III. PLAINTIFF'S INTERPRETATION OF BIPA IS BARRED BY SECTION 230 OF THE COMMUNICATIONS DECENCY ACT.

Section 230 of the CDA provides that "no cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with" Section 230. 47 U.S.C. § 203(e)(3). Specifically, Section 230 creates immunity from liability for "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of

action, as a publisher or speaker (3) of information provided by another information content provider." *See Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100-01 (9th Cir. 2009), *as amended* (Sept. 28, 2009). Under the Ninth Circuit's *Barnes* test, "when a plaintiff cannot allege enough facts to overcome Section 230 immunity, a plaintiff's claims should be dismissed." *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (9th Cir. 2019) (affirming dismissal under Rule 12(b)(6) pursuant to Section 230.)

The first prong of the *Barnes* test is met in this instance because Plaintiff alleges AWS and Amazon are providers of an interactive computer service in the form of cloud services. The statute defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet" 47 U.S.C. § 230(f)(2). This definition substantively mirrors Plaintiff's allegation that AWS and Amazon provide "hosting, storage, and delivery of [Take-Two's] games and player data to Internet-connected gaming platforms such as Xbox, PlayStation, Nintendo, and Personal Computers." Am. Compl. ¶ 9.

Courts have adopted a broad interpretation of whether a plaintiff's claims treat an entity as a "publisher or speaker" for purposes of the second prong of the *Barnes* test. *See Doe v. Grindr Inc.*, Case No. 2:23-cv-02093-ODW (PDx), 2023 WL 9066310, at *3 (C.D. Cal. Dec. 28, 2023) ("The broad construction accorded to [S]ection 230 as a whole has resulted in a capacious conception of what it means to treat a website operator as the publisher or speaker of information provided by a third party." (*quoting Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 19 (1st Cir. 2016).)) The Ninth Circuit's ruling in *Barnes* recognizes that "many causes of action might be premised on the publication or speaking of what one might call 'information content." *Barnes*, 570 F. 3d at 1101. A court must therefore look to "what the duty at issue actually requires:" *i.e.,* "whether the duty would necessarily require an internet company to monitor third-party content." *HomeAway.com, Inc.*, 918 F.3d at 682.

The second prong is met because Plaintiff here would require Amazon and AWS, as interactive computer services, to monitor the third-party content collected and stored on AWS servers. The duties Plaintiff seeks to impose under BIPA directly implicate AWS's obligations

towards the information content of third parties. Simply put, "any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230." *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1170-71 (9th Cir. 2008).

Finally, the third prong of *Barnes* is met because the alleged biometric information at issue is—as Plaintiff now concedes—collected, generated, and provided by Take-Two. Plaintiff no longer alleges any role by AWS or Amazon in the collection or computation of the information content at issue, which places this matter squarely within the immunities of Section 230. *See, e.g., Schneider v. Amazon.com*, 108 Wash. App. 454, 467 (2001) (dismissing defamation claim under Section 230 where Amazon was not responsible for creating or developing the speech at issue.) Plaintiff's allegations may be dismissed on this basis. *See Grindr Inc,* 2023 WL 9066310, at *8 (granting motion to dismiss pursuant to Section 230 immunity); *Newton v. Meta Platforms Inc.*, Case No. 23-cv-00116-JD, 2023 WL 5749258, at *1 (N.D. Cal. Sept. 6, 2023) (same); *Ginsberg v. Google Inc*., 586 F. Supp. 3d 998, 1006 (N.D. Cal. 2022) (same); *Bride v. Snap Inc.*, Case No. 2:21-cv-06680-FWS-MRW, 2023 WL 2016927, at *8 (C.D. Cal. Jan. 10, 2023) (same).

Congress passed Section 230 with the express policy goal of promoting the continued development of the Internet and interactive media while preserving the digital free market "unfettered by Federal or State regulation." 47 U.S.C.A. § 230(b)(2). It is fully consistent with Congressional intent to invoke Section 230 where a plaintiff would extend BIPA beyond its rational application to create onerous liability for providers of interactive computer services. Holding cloud service providers responsible for BIPA compliance with respect to third-party data would create an extensive burden without any realistic way to comply with the statute. Nothing suggests the Illinois legislature intended that absurd result. The General Assembly focused on collection to biometrics through business interactions, such as "at grocery stores, stores, gas stations, and school cafeteria." 740 ILCS 14/5(b). These are point-of-sale and point-of-services transactions, not tenuous two-steps-removed chains. BIPA cannot be read to require a cloud service provider to go through the impossible task of identifying individuals from whom the provider's enterprise customers collect biometric data and: (1) create a policy to delete its

enterprise customers' data (as would be required under Section 15(a)); (2) provide notice to and obtain consent from individuals ***before*** those enterprise customers collect data and store it in the cloud ((as would be required under Section 15(b)); or (3) obtain consent directly from individuals ***before*** transmitting its enterprise customer data in accordance with its contractual obligations to enterprise customers (as would be required under Section 15(d)).

Moreover, taking Plaintiff's argument to its logical conclusion, cloud email providers like Gmail and Hotmail and cloud storage companies like Dropbox could be held liable under BIPA for any biometric data stored on their servers, even if they know nothing about the data. For example, under Plaintiff's theory, if an email user sent a scan of his fingerprints by email, the email provider would "possess" that data under BIPA, creating BIPA liability even though they are completely unaware of the presence of that data. That is an absurd outcome. Moreover, Plaintiff's ill-fated reasoning is not limited to digital architecture. Under Plaintiff's same theory, parcel delivery services such as FedEx and UPS would be liable under BIPA every time they carry a package that contains biometric data, such as fingerprint records, or temporarily store that package at a distribution facility—even if FedEx or UPS has no idea what is in the package. Nothing in the language of BIPA suggests that the legislature intended to impose onerous liability on unwitting third-party vendors.

BIPA does not apply where, as here, a cloud service provider has no feasible means of identifying and contacting those whose biometric information was collected and stored in the cloud. "[I]t would be patently unreasonable to construe BIPA "to require notice to and consent from individuals who were "total strangers." *Zellmer v. Facebook, Inc.*, Case No. 3:18-cv-01880-JD, 2022 WL 976981, at *3 (N.D. Cal. 2022).[10] Section 15(b) requires a private entity to give prior notice to and obtain prior consent from the "subject." 740 ILCS 14/15(b). This requirement regulates businesses that directly collect biometric information from employees, customers, or site visitors. Section 15(b) cannot be read to impose onerous research and notice requirements on cloud storage providers whose role starts and ends with providing data storage services to enterprise

[10] The Ninth Circuit heard argument on the appeal of *Zellmer* on February 7, 2024.

customers. To the contrary, the Illinois Supreme Court has emphasized that "compliance" with BIPA "should not be difficult." So that "whatever expenses a business might incur to meet the law's requirements are likely to be insignificant." *Rosenbach*, 129 N.E.3d at 1207.

The BIPA "compliance" Plaintiff demands isn't just difficult but practically impossible, to the point where application of Section 15(b) would be absurd. Nothing in the Amended Complaint alleges any relationship between Plaintiff and AWS or Amazon; Take-Two is at all times an intermediary that has a direct relationship with its NBA2K players. Plaintiff further concedes that Take-Two provided disclosures and required consent from Plaintiff prior to collecting the alleged biometrics. Am. Compl. ¶ 96. The benefit of requiring a secondary disclosure, from an entity that does not even control the data at issue, pales against the implausible prospect of a cloud service provider policing the contents of trillions of customer files to determine whether they contain biometric information covered by BIPA. Imposing such a requirement would create a host of other privacy issues surrounding customer data that would result in actual risks to Illinois consumers. Section 230 was crafted specifically to prevent the encroachment of such onerous state-law liability onto interactive computer service providers for matters involving the monitoring of third-party data. AWS and Amazon are entitled to the protections of Section 230 here, and Plaintiff's claims should be dismissed.

CONCLUSION

For the reasons set forth in above, Defendants respectfully request that the Court dismiss Plaintiff's First Amended Complaint.

Dated: March 15, 2024

Respectfully submitted,

FENWICK & WEST LLP

By: */s/ Brian D. Buckley*
Brian D. Buckley, WSBA No. 26423

401 Union Street, 5th Floor
Seattle, WA 98101
Telephone: 206.389.4510
Facsimile: 206.389.4511
Email: bbuckley@fenwick.com

MORGAN, LEWIS & BOCKIUS LLP

By: */s/ Elizabeth Herrington*
Elizabeth B. Herrington, IL #6244547
(admitted *pro hac vice*)

110 North Wacker Drive
Chicago, IL 60601-5094
Telephone: (312) 324-1000
E-mail: beth.herrington@morganlewis.com

Attorneys for Amazon Defendants

CERTIFICATE OF CONFERRAL

Pursuant to the Court's Chambers Procedures, I certify that I conferred with Plaintiff's counsel in an attempt to avoid the necessity of this motion but the parties were unable to agree.

Dated: March 15, 2024.

MORGAN, LEWIS & BOCKIUS LLP

By: /s/ Elizabeth Herrington

Elizabeth B. Herrington, IL #6244547
(admitted *pro hac vice*)
110 North Wacker Drive
Chicago, IL 60601-5094
Telephone: (312) 324-1000
E-mail: beth.herrington@morganlewis.com

Attorneys for Amazon Defendants

LCR 7(E) WORD-COUNT CERTIFICATION

As required by Western District of Washington Local Civil Rule 7(e), I certify that this memorandum contains 7,329 words.

Dated: March 15, 2024.

FENWICK & WEST LLP

By: /s/ Brian D. Buckley
Brian D. Buckley

Attorneys for Amazon Defendants